FedRAMP Vulnerability Scanning Requirements

Version 1.0

March 20, 2018

FedRAMP

DOCUMENT REVISION HISTORY

DATE	VERSION	PAGE(S)	DESCRIPTION	AUTHOR
03/20/2018	1.0	All	Initial document that replaces FedRAMP JAB P-ATO Vulnerability Scan Requirements Guide	FedRAMP PMO

ABOUT THIS DOCUMENT

This document has been developed to provide guidance on vulnerability scanning policy, procedures, and tools in support of achieving and maintaining a security authorization that meets the Federal Risk and Authorization Management Program (FedRAMP) requirements.

Some Cloud Service Providers (CSPs) may need to transition from their current vulnerability scanners or work with their vendors in order to meet the revised requirements.

This document is not a FedRAMP template – there is nothing to fill out in this document.

This document uses the term *authorizing official (AO)*. For systems with a Joint Authorization Board (JAB) provisional authorization to operate (P-ATO), AO refers primarily to the JAB unless this document explicitly says *Agency AO*. For systems with a FedRAMP Agency authorization to operate (ATO), AO refers to each leveraging Agency's AO.

WHO SHOULD USE THIS DOCUMENT?

This document is intended to be used by CSPs, Third Party Assessor Organizations (3PAOs), government contractors working on FedRAMP projects, and government employees working on FedRAMP projects.

HOW TO CONTACT US

Questions about FedRAMP or this document should be directed to info@fedramp.gov.

For more information about FedRAMP, visit the website at http://www.fedramp.gov.

TABLE OF CONTENTS

1. PURPOSE

Continuous Monitoring (ConMon) ensures CSPs continuously maintain the security of their FedRAMP-authorized systems by providing the Joint Authorization Board (JAB) and Authorizing Officials (AOs) monthly insight into the security posture of the system. CSP scanning policies, procedures, and tools (including vulnerability scanners) are key components to ConMon activities. In an effort to increase the efficiency and effectiveness of ConMon activities, the FedRAMP Program Management Office (PMO) is instituting guidance for scanning requirements. This document summarizes the updated requirements and the immediate path forward for implementation.

2. BACKGROUND

The vulnerability scanning requirements are part of the FedRAMP Continuous Monitoring Strategy Guide and the appropriate FedRAMP Low, Moderate, or High Security Control baselines, specifically in control RA-5.

The ConMon scanning requirements move FedRAMP ConMon activities toward efficiencies, advance the quality of ConMon information provided to FedRAMP, and better position FedRAMP to perform robust analysis in the near future. These changes also better enable FedRAMP to scale up as the volume of FedRAMP-authorized systems continues to increase.

Further, FedRAMP has an obligation to determine and enforce CSP compliance with such security requirements.

3. SCANNING REQUIREMENTS

Scanning requirements are also outlined in the FedRAMP Continuous Monitoring Strategy Guide and the FedRAMP Low, Moderate, and High Security Control baselines.

This document expands on the original requirements:

- **Scanner Resiliency:** Scanners should be hardened to resist unauthorized use or modification (i.e., unnecessary ports and/or unnecessary services should be closed).
- **Authenticated Scanning**: For Moderate and High systems, the CSP must ensure authenticated scans are performed wherever possible. [RA-5(5)]
- **Scanning with Full Authorization**: For all Moderate and High systems, the CSP must ensure that scans are being performed with full system authorization. [RA-5(5)]
    - Scanning must avoid typical lack of authorization issues (including lack of access to remote registry, limited registry access, limited file access, etc.).
- **Machine-Readable Findings**: The scan output must display all scan findings with a low risk or higher in a structured, machine-readable format (such as XML, CSV, or JSON).

- If the scanner is able to output/export findings in more than one machine-readable format, the CSP must select the format that provides the greatest amount of information.
    - Where possible, the machine-readable data must include the authentication and authorization status of the scans to demonstrate the degree to which an authenticated scan was performed on each host.

- **National Vulnerability Database (NVD)**: For any vulnerability listed in the latest version of the National Institute of Standards and Technology (NIST) NVD, the Common Vulnerabilities and Exposures (CVE) reference number must be included with the machine-readable findings data for that vulnerability.
- **Common Vulnerability Scoring System (CVSS) Risk Scoring**: For any vulnerability with a CVSSv3 base score assigned in the latest version of the NVD, the CVSSv3 base score must be used as the original risk rating. If no CVSSv3 score is available, a CVSSv2 base score is acceptable where available. If no CVSS score is available, the native scanner base risk score can be used.
- **Configuration Settings**: The CSP must provide machine-readable evidence that the scanner's configuration settings have not been altered from the 3PAO-validated configuration settings approved during the initial authorization assessment.
- **Configuration Changes**: If a scanner configuration change is required (above and beyond normal patching and updates) the AO must be notified and approve of the change.
- **Signature Updates**: For each deliverable, The CSP must update the list of vulnerabilities scanned to the latest available list. [RA-5(2)]
    - The CSP must use a vulnerability scanner that checks for automatic signature updates of the scanner's vulnerability database at least monthly.
    - The CSP must provide automated machine-readable evidence of the most recent update performed prior to scanning.
- **Adequate Asset Identification**: The scanner findings must contain unique asset identifiers that map to an inventory.
    - The CSP must have an automated mechanism to identify and catalog all assets within the authorization boundary every month in order to ensure that everything is being scanned appropriately
    - For web scans, a dynamically updated catalog of web services should be maintained to include the ports where web services reside.
- **Types of Scans**: CSPs must scan operating systems, web applications, and databases monthly. All scan reports must be sent to the AO/JAB monthly. [RA-5]
    - The entire inventory (or approved sampling percentage) within the boundary must be scanned at the operating system (OS) level at least once a month.
    - All web interfaces and services (or approved sampling percentage) must be scanned.
    - All databases (or approved sampling percentage) must be scanned, including those required to support the infrastructure.

- **Plan of Action and Milestones (POA&M) Entries**: The CSP must track each unique vulnerability as an individual POA&M item.
  - Individual vulnerabilities must be based on the scanning tool's unique vulnerability reference identifier (ID).
  - The CSP may break a unique vulnerability into multiple POA&M items, such as for a vulnerability that applies to different asset types that will be remediated in different ways.
  - The CSP must not group multiple unique vulnerabilities into a single POA&M item.
- **All Non-Destructive Detections**: The CSP must enable all non-destructive detections within the scanner.
- **Image Scanning**: Where the CSP offers services, such as virtual images, and where the customer is responsible for scanning but is reliant on the CSP for patching, the CSP must scan the source image for all available customer leveraged images.
  - This applies to all images in use or available for use by Federal customers.

These requirements ensure AOs are able to provide high-quality ConMon oversight across a CSP's system and ensures consistency in scan results for AOs to analyze across multiple systems.

Only scanning tools that meet the revised requirements will be accepted by FedRAMP for ConMon. This may impact the current ConMon strategy of some CSPs. The FedRAMP PMO can assist CSPs to determine if other scanners are able to meet FedRAMP requirements.

4. TRANSITION PLAN

CSPs should be using only approved and compliant scanners. These requirements are effective immediately, and CSPs must be fully compliant by September 1st, 2018.

For those CSPs that anticipate being unable to meet the September 1st, 2018 deadline, FedRAMP requires justification and a plan of actions detailing how and when the CSP will be using compliant scanners. Alternatively, AO's can work with CSPs on a specialized plan to implement specific mitigations. Either way, the CSP will need to inform their AO, by May 31st 2018, regarding when they plan to be fully transitioned to scanners that meet all of the new requirements above.

CSP plans for late implementation or mitigation must provide clear justification and will be reviewed and approved by their AO. For those CSPs currently authorized through the JAB Provisional Authorization to Operate (P-ATO) process, the JAB will be tracking the CSP's scanning requirements implementation or mitigation status in their monthly ConMon reports and reviews. Any CSPs currently authorized by agency authorizations will need to consult with their AOs, and likely will be required to add a scanning requirements plan of action to their POA&M.

Operating with only up-to-date approved ConMon scanners will be a FedRAMP requirement moving forward; therefore any CSPs not yet approved will be informed of this requirement.

APPENDIX A: FEDRAMP ACRONYMS

The *FedRAMP Master Acronyms & Glossary* contains definitions for all FedRAMP publications, and is available on the FedRAMP website Documents page under Resources Documents.

(https://www.fedramp.gov/documents/)

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.

APPENDIX B: GLOSSARY

Asset: A physical or virtual device or component within an information technology system, identified by a unique asset ID.

Authentication: A scanning tool's ability to log in with administrative privileges on an asset in order to perform a scan with elevated privileges.

Authorization: A scanning tool's ability to access the registry and files on an asset remotely in order to perform a full scan.

Detection: An individual program within the scanning tool that checks for a given vulnerability or other data point (authentication, etc.) that is flagged as a finding, identified by a unique detection ID.

Vulnerability: A scan detection that relates to a specific weakness, identified by a unique vulnerability ID.